THE DIFC DATA PROTECTION LAW – PROPOSED AMENDMENTS

INTRODUCTION

In June 2019, the Dubai International Financial Centre ("**DIFC**") issued a public consultation on its proposed new Data Protection Law (the "**Proposed Law**"). The Proposed Law will replace the 2007 DIFC data protection law (as amended) (the "**2007 Law**") and aligns the DIFC's regulatory framework more closely with international data protection developments, including the General Data Protection Regulation ("**GDPR**").

Clifford Chance provided comments to the DIFC on the Proposed Law and in this briefing we note some of the salient features of the Proposed Law that will affect the data processing operations of companies operating in the DIFC.

Whilst the law that is finally enacted may differ from the Proposed Law, we anticipate that these key concepts will be retained. We regularly advise corporates on compliance with the GDPR and DIFC data protection laws and can help your business navigate these changes.

Extra-territorial reach?

One of the most significant aspects of the GDPR is its extra-territorial effect in monitoring data processing activities anywhere in the world that have certain connections with the EU. While the Proposed Law does not go as far as the GDPR in regulating entities outside the DIFC, a DIFC company that outsources its data processing activities to a company outside the DIFC is now required to enter into a formal contract (with certain mandatory provisions) with the non-DIFC data processing company.

This is a concept from the GDPR and, under the Proposed Law, commencing data processing without such a contract is a breach of the law. The DIFC acknowledges that many DIFC companies may not have such contracts in place and therefore it is likely that the Proposed Law will allow for a grandfathering period for companies to enter into such contracts.

Emphasis on self-regulation

There is a greater emphasis on self-regulation in the Proposed Law, which replaces the need for the DIFC Data Protection Commissioner's consent for certain activities. Equally (compared to the 2007 Law), data subjects have additional rights in line with the GDPR which allows for an eco-system of self-regulation in the DIFC.

An example of such self-regulation is in the context of joint controllers, where two or more controllers of personal data are required to agree their respective responsibilities.

Key Changes

- Requirements for processing data outside the DIFC
- Emphasis on self-regulation
- Stricter consent requirements
- Impact on transfers
- Data Protection Officer and Data Protection Impact Assessment
- More rights for data subjects

Stricter consent requirements

The requirement to obtain the data subject's consent prior to processing, which existed under the 2007 Law, has been retained. However, the Proposed Law adopts a more stringent approach to what may, or may not, constitute consent and requires controllers to assess the validity of the consent periodically. The Proposed Law gives detailed requirements for consent that processors and controllers must adhere to so as to ensure consent is freely and unambiguously given in respect of each specific data processing purpose, thus distinguishable from consents obtained for other purposes. We expect that silence, pre-ticked boxes and inactivity might not constitute consent under the Proposed Law.

Impact on data transfers

As per GDPR and the 2007 Law, the Proposed Law has retained the concept of permitting data transfers to pre-approved jurisdictions "with an adequate level of protection" (i.e. jurisdictions with sufficiently robust data protection regimes, which will be listed on the DIFC website). However, in the context of transfers to jurisdictions without an adequate level of protection, and in line with the greater emphasis on self-regulation, the Proposed Law provides processors and controllers with a larger array of options than the 2007 Law. In particular, the Proposed Law permits transfers to such jurisdictions where the processor/controller deems that adequate safeguards are in place, directed by the detailed guidance in the Proposed Law as to what constitutes "adequate safeguards".

The Proposed Law also allows controllers to have Binding Corporate Rules approved by the Data Commissioner which permit intra-group transfers. Alternatively, intra-group transfers could occur under the legitimate interest ground.

High Risk Processing Activities

The Proposed Law introduces the concept of "High Risk Processing Activities" which are noted below with our suggested examples:

- the use of new technology that increases risk to Data Subjects (e.g. the use of artificial intelligence or machine learning);
- the processing of a "non-trivial" amount of special categories/sensitive personal data (e.g. race, health, religion, etc.) (e.g. healthcare and insurance providers);
- processing large amounts of Personal Data that poses a high risk to the Data Subject, for example, on account of sensitivity of Personal Data (e.g. data processor companies including cloud storage companies); or
- automated processing, including profiling, which leads to decisions with legal effects on natural persons (e.g. online recruitment tools without human intervention).

A processor or controller that engages in High Risk Processing Activities must adopt a more cautious approach to processing. The Proposed Law requires such companies to carry out regular data protection impact assessments ("**DPIAs**") and to appoint a data protection officer ("**DPO**") before proceeding. Significantly, the onus will be on the processor/controller itself to assess whether an activity carries sufficient risk to warrant such steps. It is possible that the final law will provide more clarity on when a DPIA or DPO will be required but these concepts, stemming from the GDPR, are likely to be retained.

Key New Concepts

- ***Binding Corporate Rules*** - written procedures which regulate the transfer of personal data between members of the same group. Binding Corporate Rules are an avenue for intra-group transfers of personal data out of the DIFC.
- ***High Risk Processing Activities –*** activities that have a greater chance of making personal data vulnerable to unintended disclosure and therefore require additional protections including, conducting a data protection impact assessment and appointing a data protection officer.
- ***DPO -*** *data protection officer to monitor compliance with the Proposed Law. International Groups can rely on DPOs in their network.*
- ***DPIA –*** *data protection impact assessment – international groups can rely on DPIA's conducted in their network if such DPIA's cover the requirements stipulated in the Proposed Law.*

DPO obligations

As noted above, processors or controllers engaging in "High Risk Processing Activities" are required to appoint DPOs. The DPO must ordinarily be resident in the UAE. However, international groups can appoint a single DPO based outside the UAE provided they can fulfil their functions under the Proposed Law. We anticipate that most international groups may rely on their DPOs in the wider network (e.g. the EU). Care should be taken to ensure the DPOs have sufficient and regular training on DIFC data protection law.

DPOs will also be required to monitor their company's compliance with any data protection provisions to which the company is subject. This is likely to give rise to challenges for DIFC processors/controllers and their respective DPOs, as they will be required to understand, and keep track of, an array of potentially contrasting foreign regulations impacting their organisations. We expect that the DIFC will provide further guidance on this requirement.

DPIA requirements

Controllers engaging in "High Risk Processing Activities" shall also be required to carry out DPIAs. In the EU, DPIAs are not required under the GDPR where processing is not on a large scale, such as in the case of processing personal data from patients or clients by healthcare professionals or lawyers. The DIFC may clarify if such an exemption will exist under the Proposed Law.

The Proposed Law sets out detailed guidance on the form such DPIAs must take and includes a requirement to consult with data subjects, if appropriate, in the preparation of DPIAs.

Where a DIFC controller is part of an international group, and another entity in that group has conducted a DPIA which is compliant with the Proposed Law, the DIFC controller may rely on that DPIA for the purposes of adhering to the Proposed Law.

Rights of data subjects

As is the case with the 2007 Law, the rights of data subjects remain a core component of the Proposed Law, with many of the new concepts clearly intended to reinforce the protections surrounding such rights.

Under the Proposed Law, the list of data subject rights has been expanded. In particular, data subjects shall now have an express right to withdraw consent at any time, as well as the right not only to object to processing, but also to restrict processing in certain circumstances.

Following the implementation of the GDPR in the EU, there was a notable increase in data subject access requests. In the DIFC, the access request right existed under the 2007 Law. However it remains to be seen if the Proposed Law leads to a similarly significant increase in such requests in the DIFC. Companies may need to create systems to deal with such requests which can be quite an extensive exercise.

Conclusion

The Proposed Law heralds some significant operational changes for DIFC Companies who may have to review existing data processing arrangements, update data policies and consent forms, appoint a DPO and conduct a DPIA on a regular basis. For further assistance, please contact James Abbott or Arun Visweswaran.

Additional Rights for Data Subjects

- Right to withdraw consent at any time
- Right to restrict processing in certain circumstances
- No discrimination against a data subject who exercised rights
- No decision affecting data subject based solely on automated process
- More information to be provided by data controllers/processors
- "**Profiling**" – automated evaluation of personal aspects of a natural person (such as to assess work performance, economic situation, health, behaviour, movements and personal preferences). Specific restrictions under the Proposed Law on automatic profiling.

CONTACTS

James Abbott
Partner

T +971 4503 2608
E james.abbott
@cliffordchance.com

Arun Visweswaran
Senior Associate

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

Connor Partos
Associate

T +971 4503 2664
E connor.partos
@cliffordchance.com